Responsibility and Non-repudiation in resource-constrained Internet of Things scenarios

Edewede Oriwoh, Haider M. al-Khateeb, Marc Conrad
Department of Computer Science and Technology
Institute for Research in Applicable Computing
Bedfordshire, United Kingdom
Email: {edewede.oriwoh@beds.ac.uk; haider.alkhateeb@beds.ac.uk; marc.conrad@beds.ac.uk}

Abstract **- The proliferation and popularity of smart autonomous systems necessitates the development of methods and models for ensuring the effective identification of their owners and controllers. The aim of this paper is to critically discuss the responsibility of Things and their impact on human affairs. This starts with an in-depth analysis of IoT Characteristics such as Autonomy, Ubiquity and Pervasiveness. We argue that Things governed by a controller should have an identifiable relationship between the two parties and that authentication and non-repudiation are essential characteristics in all IoT scenarios which require trustworthy communications. However, resources can be a problem, for instance, many Things are designed to perform in low-powered hardware. Hence, we also propose a protocol to demonstrate how we can achieve the authenticity of participating Things in a connectionless and resource-constrained environment.**

Keywords: Internet of Things; Characteristics; Protocol; Responsibility; Liability; Authentication; Identification; Public Key Cryptography; Cyber-Physical Environment

I. Introduction: The Internet of Things

It has been attributed a variety of labels: the *Internet of Things (IoT)* [2], the *Internet of Everything (IoE)* [5] , the *Future Internet (FI)* [6], and so on. Research and Industry have, and are still developing protocols and standards for it: *Electronic Product Code (EPC)* [24], Radio Frequency Identification (RFID) [8], *micro IP (uIP)* [15], *Routing Protocol for Low Energy and Lossy Networks (RPL)* [17], *Ad hoc On-Demand Distance Vector (AODV)* [17], *Bluetooth Embedded System (BTE)*[16] , *Bluetooth Low Energy (BLE)* [19], *Long Term Evolution (LTE) [11] and LTE-Advanced (LTE-A, i.e. 4G)*, *If This Then That (IFTTT)* [22], [3] , *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN)* [15], are some of the standards and protocols being developed for use in the IoT. *Internet Protocol version 6 (IPv6)* [12], *Mobile IPv6 (MIPv6)* [15], [14], has been developed and made available in time to enable the unique addressing of billions of nodes thus fostering and enabling the IoT. The benefits of the IoT are widely discussed in the literature.

Several companies including *Cisco* [4] among others, have talked about the potential *economic, financial* benefits (governments of Europe, China, USA, etc). The lifestyle management benefits and improvements to human life are being espoused by industry and individuals, researchers and consumers, and by governments and international conglomerates.

There is also a growing number of small companies and projects working towards IoT driven solutions: Xively (https://xively.com/), TinyOS (http://tinyos.stanford.edu/tinyos-wiki/index.php/Main_Page) [13], TransFabric, ContikiOS (http://www.contiki-os.org/) [1] are a few of them.

Among the discussions about the benefits of the IoT, potential security and privacy threats and challenges are also discussed in the literature [7], [9], [10], [21]. This paper addresses an issue which is however not gaining as much attention as the issues of confidentiality and privacy: this issue is *Responsibility* in a largely interconnected world.

Key Characteristics of the IoT are discussed in Section II; Section III briefly discusses Weiser's Vision of technologies that are indistinguishable and invisible to human agents; potential Future challenges within the IoT are presented in Section IV; Section V defines Responsibility as it relates to the IoT; Section VI-A makes some suggestions for addressing the challenges presented earlier; the novel authentication and identification protocol for resource-constrained nodes in the IoT is presented in Section VII; Section VIII discusses Future Work and concludes.

II. IoT characteristics

The IoT is a hybrid network. It is composed of software and hardware components, physical and logical entities, human and non-human nodes. It encompasses the Internet, all Machine-to-Machine systems and human-to-human interactions on social media. It adds a dimension of independence and autonomy and meshes all pre-existing network systems into a useful system of nodes and controllers. The IoT has some essential characteristics that make it a different network and justifies the attention it is receiving in academia, industry and media. These characteristics (Fig.1) are Autonomy, Pervasiveness and Ubiquity.

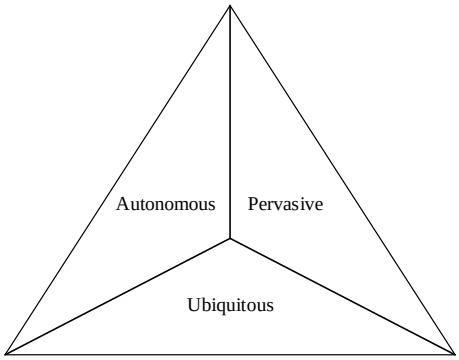

Figure 1: *IoT Characteristics Triangle*

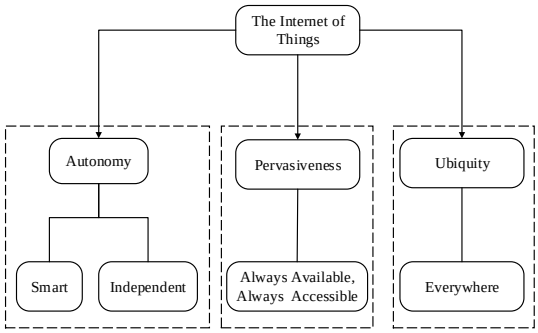

Figure 2: *Expanded IoT characteristics*

Autonomous Operation: The Characteristics of Autonomy are embodied in the ability of nodes/devices/agents to be *Smart* and to operate *Independent* of any control. This is a crucial role that the nodes in the IoT are expected to be able to deliver: independent decision-making.

Pervasiveness:Always *Available*, Always ON, Always *Accessible*. It is to be always ON such that it can be accessed readily

Ubiquity: Everywhere. Nodes or their representations (e.g. their virtual online interfaces) must be accessible from everywhere/globally accessible.

Each of these characteristics (Fig.2) can be associated directly with certain features of the IoT nodes (or devices). These features include:

Smartness: the characteristic that means a node can do much more than its less-smart counterpart;

Independent: In addition to it's advanced feature and abilities, nodes are able to operate of their own "will" so to speak;

Availability and Accessibility: IoT nodes are, of necessity expected to, through available communication links, be always within reach of their owners for control reasons or just for reasons of access e.g. to retrieve data about presences within a home environment;

Everywhere: IoT network, by its nature as the network that encompasses all other networks physical and logical, and that it includes everyday items which have the extra abilities (smartness) of communication and/or computing and/or control, this means that the physical environment however rural or urban, will become a subset of the IoT. For instance, a farmer in a remote village that

III. Weiser's Vision

In the 1991 paper, "The Computer for the 21st Century" [23] Mark Weiser presented a vision of how technology will become seamlessly integrated into human affairs and lives that the best ones will be the ones that are indistinguishable i.e. do not stand out as separate from us but form a key part of our everyday ordinary existence. This is partly what the IoT is to become: everyday and ordinary. When faced with the question about when the IoT will happen, the answer is clear because the IoT is already a part of our lives in the form of Smart devices that more and more humans are beginning to rely on for communication (Smart Phones), entertainment and connectivity (Smart Phones, Smart Televisions), transportation (Smart Cars, Drones (Amazon)), Wars and Security (Drones and Quad-copters), Games and Sports (Drones racing, Smart Shoes - Nike), Healthcare (Smart Pills, Robotic surgical arms), Community Management (Smart Cities), Customer Service (Walmart, etc.), Smart watches, smart bulbs, smart meters, smart heaters, elderly care (Smart comfort Toys) to name a few. They will continue to play more roles in our every day lives

IV. Future Challenges

We identify and present several challenges in this section. These challenges do not relate to the potential financial value of the IoT or its value to society as a system which can be used to make things better, faster, seamless and make life easier for humanity. The challenges presented here are the ones that don't appear to be gaining the attention of the stakeholder in the so-called IoT industry. A few questions are posed:

The Weakest Links?

What is the role of individuals in a highly-efficient, interconnected world. Are end users still to be seen as the weakest links in the security chain or should they be more readily referred to as the most essential and potentially, most important links in the chain? It is therefore, perhaps, time to change the narrative: The user is no longer to simply be seen as the weakest link but as the most essential link. This is because within an environment such as a Smart Home (SH),

users will be expected to have a degree of control of their homes. Users themselves will expect that even though their homes have become *smart* this would not mean they should relinquish total control of their homes. This means that a sense of overriding control over all systems in their homes including the security systems would be required by users. It must therefore be impressed upon users the importance that they maintain their sense of responsibility for their homes and the nodes within the homes.

Responsibility

Hypothesis: Humans will be at the fore-front of managing their security in their homes - just as they are today. Most people physically lock their doors and windows as a way to bolster secure and fortify their homes. They trust the devices (window and door locks) to keep then safe and separated from unwanted attention. Within the IoT/SH arena, the only difference is that people will be required to trust ubiquitous, trained, learning nodes with this task of securing the fort. What would people's response to this transference of responsibility be? Will it be one of complete offloading? Or might there be some resistance to a total transfer. The answer to this question is not derived from a survey but from an observance of natural ways of doing things. It can be anticipated that people will still hope for some kind of control over their nodes or the entire homes especially since, at their core, SH are, essentially/effectively, *homes*.

Transference of Responsibility, liability and culpability

This is one of the main challenges that Cyber-physical Systems (CPS) may be faced with. With autonomous nodes, it will be possible for node owners to train their nodes to carry out certain actions on their behalf. Should these actions result in unfortunate circumstances, for instance, causing harm to human agents, there is a potential for human agents to wish to attribute blame for the actions and consequences of the actions of smart, self-managing, decision-making non-human nodes to them. It is perhaps necessary to recognise that when damage or harm is caused by a human agent or a non-human agent, the results and feedback (for the cause of the damage or harm) are different (Table I). This transference, if not properly handled, can lead to the next identified Challenge

Legal Quandary

The laws that guide the use of autonomous nodes must be clearly spelt out especially since they are gradually becoming more and more ubiquitous

Due to the rapid evolution of the IoT, Smart Environments the legal frameworks that currently exist may need to adjust to accommodate any emergent threats and offences that occur within these systems. The law has managed to accommodate crimes such as Data Theft, Tampering, accessing another's computer or device without permission under existing laws. However, within the Cyber-physical Environment (CPE) of the IoT, the offences may be a little more nuanced

Entity	Responsibility Type	Feedback
Human	Consequential and/or Causal	Punishment, Reprimand, Re-training
non-Human	Causal	Repair, Retirement, Re-training

Table I: *Responsibility Type*

Privacy

There has been a surge in interest in the subject of Privacy especially with the recent growth of CP systems. The conflicting situations where a significant amount of unprocessed and processed data about individuals has and can be made accessible and the fact that somehow this data is required to provide certain services in CPE makes the issue of privacy an interesting one to address. Some questions raised by this conundrum include:

Irrelevant Privacy: Is there going to be such a thing? Does it matter? Is Privacy with all the attendant arguments, now irrelevant and if it is, should we be concerned?

Relative Privacy: It is essential to bear in mind that what is deemed private information to you may be open to share with someone else. Who decides what is best kept private per person/individual? Is it ONLY what they have power over? Take as an example, the public use of Closed Circuit Television (CCTV) technology. If you don't want anyone to know that you left your house today - i.e. you use the back door to avoid saying hello to friends because you feel unwell, for instance- what gives a CCTV operator the right to breach that personal requirement by recording the fact that you actually physically stepped out of your home. Are you implicitly guilty because you want to be let alone?

At present a huge amount of data is being freely made available by individuals on the Internet and other connected forums. However, it must be recognised that among the population samples, there are those who share their details sparingly, if at all. There is, indeed, a proportion of the world's populace that does not necessarily deem it important to beam out to the world, in minute detail, what you had for breakfast, lunch, what came up and then what you had for dinner. What rights do these people have in a fully-developed Cyber-physical Environment?

In the event that service providers (traffic management, electricity companies, home security solution providers) start to manipulate (collect, analyse and process) our data in order to study us and provide us ever-improved services, what choice do we have in deciding what we want to share and what we do not want to share? This data, however "anonymised", can be used to build a profile of users and this profile, if closely-matched to other collected data that may at first appear random, can be used to draw a picture of the everyday activities of individuals.

These are just some areas that we might wish to ponder as we enjoy the emergence of an interconnected world.

V. Responsibility Defined

Responsibility is defined severally by the Oxford Dictionaries website (http://www.oxforddictionaries.com/definition/english/responsibility) as

"the state or fact of being accountable or to blame for something." (**human responsibility?**) or

"a moral obligation to behave correctly towards or in respect of" (**non-human responsibility e.g. of a robot?**).
It is also defined as

"a thing which one is required to do as part of a job, role, or legal obligation"

and lastly as

"The opportunity or ability to act independently and take decisions without authorization" (**again, non-human responsibility?**)

These definitions highlight the fact that within the IoT, there will be different kinds of responsibility and that it may be possible to attribute responsibility for certain "events" to non-human agents.

VI. Discussion

A. Present Solutions

1) Awareness: As robots become increasingly commonplace, one suggestion for ensuring a smooth transition to this era is through clear information to introduce users to the presence of non-human nodes which perform the services in place of humans. With autonomous, non-human agents such as robots, we mustn't be afraid - but we must be aware. In the case of stores that have non-human agents performing the duties of humans, at the very least, it must be made known to the public that the store uses human-like robots.

Bearing in mind that *Things* can be Physical or Logical, tangible or intangible, and that they can be controlled by direct physical touch, remote control and self-learned, self-taught action (see Fig.3), the following Thing Commandments are suggested by [18]. These are not hard and fast rules. They are simply recommendations that might be adopted wholly or as separate unites depending on requirements.

2) The Thing Commandments: A set of Commandments are herein presented.

Responsibility for Things and their actions
One of the characteristics of Things in the IoT as identified in Fig.1 is **Autonomy**. Autonomy can be described as independent action and decision-making. Things may act or be caused to act in several different ways (Fig.3): based on actions initiation directly a user e.g. light switch being flipped manually; remotely e.g. turning a light bulb ON from outside a home using a mobile phone connected to the Internet; and lastly, via "learned" control: a user can set up their home network such that the lights come on at a particular time. The home system then observes the user's behaviour until they (the lights) learn to switch their state to on at the right time of the day. In the case where the device has learned the user's routine (or has been *programmed*) and it comes ON at a particular time, this action is the responsibility of whom? It is not obviously the user's because of the inherent fact that humans are not wholly predictable and even those who have a pattern can deviate from their patterns should the need arise. Are humans now to be criticised for being human?

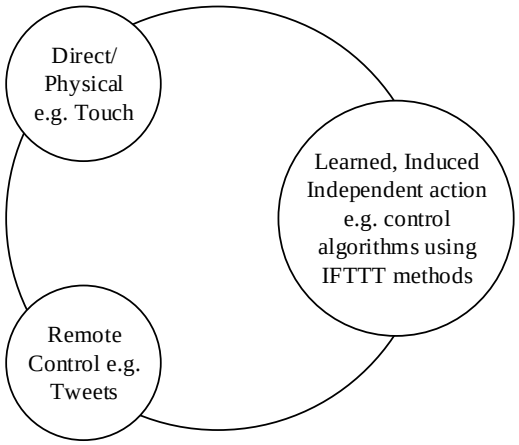

Figure 3: *Controlling Smart Things*

Picture a landscape with driver-less cars, drones i.e. non-human agents interacting independent of human control and observation. In such an environment it will be essential to remember the first Thing Commandment - "Your Thing is Your Thing" and, therefore your Responsibility.

Illegal Access
Access people's non-human nodes without permission must still be deemed improper behaviour. This is especially important in the CP Environment of the IoT where modes such as drones can be taken control of by rogue controllers and used for malicious purposes.

Relationships between Things
Things owned by a user should have an identifiable relationship with each other. The method of polling each other or having logical or even physical markers may prove invaluable in situations where a node has turned up in an unexpected environment (see http://www.telegraph.co.uk/news/worldnews/europe/france/11458116/Drone-spotted-over-French-military-site.html). If a drone is abandoned by a - possibly panicked - owner, or even deliberately, it will be essential for law enforcement agencies to be able to identify the node's owner and most recent controller.

Authenticated Communication
Things owned by a user should have be able to identify communication between with each other. This can be achieved - and is already being achieved - through the use of existing and future authentication mechanisms.

Usability and Ease of Use
This commandment discusses how nodes designed for use as part of a CPE must be easy to control and use by end users. If this commandment is not applied then there is a risk that systems may be too complicated for users and that companies may exploit the relative lack of knowledge of people to charge them for installations. It must be recognised that just because a person is buying a smart car/television/fridge does not mean they should be expected to sit through hours of training on how to adapt to using these new systems. The transfer should ideally be seamless and practically invisible to users [23].

Control
All things should be controllable by their owners
Control their physical and logical behaviour. This will be used to avoid trojan Horse defences. the users should recognise the potential for them to be the culprits or liable.

Ownership
Things must have owners. Everything must have an owner that is clearly and readily identifiable. A marker or label on the things which can be accessed readily is one way to meet this requirement. Another is through the use of logical markers e.g. bar codes that can be scanned to reveal ownership, unique identifiers such as Media Access Control (MAC) addresses on Network Interface Cards (NIC) cards

Inverse ownership relationship
The use of smart nodes promise to apparently improve the way things are done and make things easier for humans thereby affording them more time to concentrate on things that they deem more important. A car and public traffic system that decide the best and fasted route to work are a good option and a driver of such a car may choose to then take that route and not worry about getting to work late due to traffic. However, it essential for human agents to have a choice about whether they wish to own or use autonomous nodes or not. This commandment simply proposes the notion that Not everyone needs to own Things.

Freedom From Things Refusing, disabling and destroying or disposing of Things.
Humans should be free to get rid of nodes that they no longer require. A non-human node may be disposed of at the user's discretion even if the non-human has a human-like form. A *kill switch* - a remote or local physical button - on a robot will therefore be essential. The decision to stop a robot offending will be deemed the responsibility of the owner or controller of the robot where these can be one and the same individual or more than one entity.

B. Best Mistakes

There are undoubtedly going to be teething issues including in areas of security, privacy, damage, and loss. However, among these, there will be issues that are in this section referred to as *mistakes*.

1) Attributing Responsibility is not an important issue: This appears to be the status quo currently with the deployment of Smart Nodes and devices. There does not seem to be any coherent effort geared towards recognising the roles, responsibilities and expectations from human agents in their use, ownership and association with smart, autonomous non-human nodes (see http://edition.cnn.com/2015/04/15/politics/aircraft-lands-on-capitol-grounds/).

For reasons already discussed, it is important to be able to identify owners or at least agents who may have remote and/or local access to autonomous nodes. This includes nodes such as personal/recreational drones.

One solution is presented in Section VII where one method of establishing trusted communication between nodes is discussed.

One way would be for Things to always poll their owners (or current controllers) and vice-versa when they are ACTIVE. This way, if an attacker takes over control of a node which is programmed to poll its current controller, then whoever has control of the node can be identified.

2) If all else fails, blame the robots: Or, perhaps not.

The biggest mistake that will be made in the IoT will be to lay comprehensive blame and responsibility for faults on intelligent, independent, autonomous non-human agents. This will be detrimental to their purpose. Whatever decisions autonomous machines make will be made within the realm of what their creators "identify" as good decision-making unless(that is, of course,until they are granted the capabilities to make independent, original decisions not influenced by *prior* information). But then, what will be the point of having robots? The intention is for them to "serve" a purpose. This therefore means that we have to influence the way they think by infludencing their behaviours and habits with prior knowledge of what we consider to be right and what we deem to be wrong. This can be, at first, a set of simple rules. After this, we will need to introduce them to what, for instance, a convenience store manager considers good and what she deems to be wrong by allowing the robot to observe and learn from other store staff as well as the store's customers.

VII. Resource-Constrained Authentication Protocol (ReCAP)

In response to the challenges of ownership, identification, authentication and *non-repudiation*, we propose that these core security requirements must be realised at the design level. Any IoT device that is able to initiate or respond to communication can also include embedded security at the manufacturer following an approach similar to the Trusted Platform Module (TPM), currently used to secure hardware [20]. However, if TPM is adopted, it can be resource consuming if applied directly to offer facilities to low-power and resource-constrained IoT systems. TPM has been designed to support many security features such as verifying device integrity and examining whether the existing configuration of a device has been altered since the last session or not. In our work, we scope our objective at the essential requirement of providing means to identify each device and support sufficient authentication and integrity check in a connectionless environment using Public Key Cryptography (PKC). In a connectionless environment each message (e.g. a control command to the IoT device) is transmitted separately, there is no conversation (or session) initiated between the two communicating parties

We argue that, Things must always include an integrated PKC key pair to achieve mutual authentication, further to the security advantage of the design, the device will not be required to support any extra functions to perform key generation. Overall, to support our protocol, the IoT device should:

- Include an embedded key pair (Public/Private keys), the private key must be secured and protected.
- Memory space to store an external Public key (from a server)
- A static ID

Realising security for Things must be fast, the number of required connections must be reduced to the least and the application must not rely on the availability of third parties such as Certificate Authorities (CA). After all, CA can not easily exist for resource-constrained infrastructure.

The following steps demonstrate how the ReCAP protocol works in a Smart Home scenario; the notations used are explained in Table II.

A. Registration

SH-d registration with SH-s:

SH-d $\longrightarrow$ SH-s: ID_{SH-d}, PUB_{SH-d}, T_{SENT}, SIG_{SH-d}

Where,

SIG_{SH-d} = [h (ID_{SH-d} | PUB_{SH-d} | T_{SENT})]

...

$\mathrm{SH}_S \longrightarrow \mathrm{SH}_D$: ID_{SH-s}, PUB_{SH-s}, T_{SENT}, SIG_{SH-s}

Where,

SIG_{SH-s} = [h (ID_{SH-s} | PUB_{SH-s} | T_{SENT})]

The implementation of ReCAP requires a server. The server will act as a proxy which dictates all communications between the device and the outside world and documents every interaction in log files to support the work of Incident Responders and Digital Forensics Investigations. Registration is mandatory when the device is connected for the first time. The device registers its ID and shares its Public key with a dedicated server. These values are sent with a signed hash to maintain the integrity of the information shared. Time is included in the hash for synchronisation purposes and to realise the time this transaction was first initiated. This could also prevent replay attacks.

B. Authentication

(i) Authenticating messages from SH-s to SH-d:

SH-s $\longrightarrow$ SH-d: ID_{SH-d}, M_{SH-s}, T_{SENT}, SIG_{SH-s}

Where,

SIG_{SH-s} = [E_{PRI} {h (ID_{SH-d} | M_{SH-s} | T_{SENT})}]

Once the device is registered, every message communicated from the server can now be authenticated against a hash signed by the private key of the server. This is possible because the device has the public key of the server in its memory as an outcome of the one-time registration process. This mechanism maintains authenticity and non-repudiation of each message exchanged. Similarly, messages from the device to the server can be authenticated as in the following step.

(ii) Authenticating messages from SH-d to SH-s:

SH-d $\longrightarrow$ SH-s: ID_{SH-s}, M_{SH-d}, T_{SENT}, SIG_{SH-d}

Where,

SIG_{SH-d} = [E_{PRI} {h (ID_{SH-d} | M_{SH-d} | T_{SENT})}]

Notation	Description
SH-d	Smart-Home device
SH-s	Smart-Home server
ID	Unique identifier
PUB	Public key
PRI	Private key
T_{SENT}	Time
SIG	Digital signature
E_{PRI} {...}	Data encryption with a private key
h(...)	Hash function
|	Denotes concatenation
M	Message to be authenticated

Table II: *Protocol Notations*

VIII. Conclusion and Future Work

The work investigated the subject of Responsibility in Cyber-Physical Environments; while it is not currently clear how responsibility will be attributed in these types of systems, we concluded that for the sake of supporting Digital Forensics investigations, several data sources need to be made available; these sources include the network logs of node connections as well as the communication data of links between the participating nodes. Taking the extreme example of resource-constrained IoT environment, we have presented a protocol to authenticate messages. The essential requirement was to support fundamental security principles but without considering the confidentiality of data. We argued this was necessary as part of the trade-off between security and the implementation of resource-constrained Things. The ReCAP protocol demonstrates that achieving non-repudiation is feasible, which helps to establish links alongside the Cyber-Physical Environments.

Further work could be directed towards conducting a critical evaluation of the performance of different protocol implementations. For instance, the currently proposed ReCAP compared to an altered version where we attempt to maintain more security features such as confidentiality by encrypting exchanged messages.

Other research strands may be developed as part of the discussion around Responsibility in the IoT. One such strand is the development of a Legal Framework to guide the use and ownership and ethical retirement of Autonomous Systems as well as laws that can be used to try cases where autonomous, non-human, nodes independently act and cause harm and where their actions have adverse effects on human agents. This can be through a system of ***Autonomous Systems Law***, Law that deals with the investigation and prosecution of cases that involve autonomous agents e.g. robots.

References

[1] S. Anuj and Jurgen S. 6lowpan with uipv6 in contiki. *Advanced Distributed Systems Lab (320602) Tutorial Notes*, 2011.

[2] K. Ashton. That âĂŸinternet of thingsâĂŹ thing. *RFiD Journal*, 22:97–114, 2009.

[3] Luigi Atzori, Davide Carboni, and Antonio Iera. Smart things in the social loop: Paradigms, technologies, and potentials. *Ad Hoc Networks*, 18:121–132, 2014.

[4] Loucks J. Noronha A. Macaulay J. Buckalew L. Bradley, J. Internet of everything (ioe): Top 10 insights from ciscoâĂŹs ioe value index survey of 7,500 decision makers across 12 countries. Technical report, 2013.

[5] Armir Bujari and Claudio E. Palazzi. Opportunistic communication for the internet of everything. In *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*, pages 502–507. IEEE, 2014.

[6] Jan Camenisch. *Research Challenges to Secure the Future Internet*, pages 14–17. Secure Data Management. Springer, 2014.

[7] Jan Camenisch. *Research Challenges to Secure the Future Internet*, pages 14–17. Secure Data Management. Springer, 2014.

[8] Qi Chai, Guang Gong, and D. Engels. How to develop clairaudience - active eavesdropping in passive rfid systems. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*, pages 1–6, 2012. ID: 1.

[9] Yen-Kuang Chen. Challenges and opportunities of internet of things. In *Design Automation Conference (ASP-DAC), 2012 17th Asia and South Pacific*, pages 383–388. IEEE, 2012.

[10] Kim-Kwang R. Choo. The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8):719–731, 11 2011.

[11] Luca Costantino, Novella Buonaccorsi, Claudio Cicconetti, and Raffaella Mambrini. Performance analysis of an lte gateway for the iot. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*, pages 1–6. IEEE, 2012.

[12] Mathilde Durvy, Julien Abeillé, Patrick Wetterwald, Colin O'Flynn, Blake Leverett, Eric Gnoske, Michael Vidales, Geoff Mulligan, Nicolas Tsiftes, Niclas Finne, and Adam Dunkels. Making sensor networks ipv6 ready. In *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems*, SenSys '08, pages 421–422, New York, NY, USA, 2008. ACM.

[13] Philip Levis, Sam Madden, Joseph Polastre, Robert Szewczyk, Kamin Whitehouse, Alec Woo, David Gay, Jason Hill, Matt Welsh, and Eric Brewer. *TinyOS: An operating system for sensor networks*, pages 115–148. Ambient intelligence. Springer, 2005.

[14] Hero Modares, Amirhossein Moravejosharieh, Jaime Lloret, and Rosli Salleh. A survey of secure protocols in mobile ipv6. *Journal of Network and Computer Applications*, 39:351–368, 2014.

[15] Julien Montavont, Damien Roth, and Thomas NoÃńl. Mobile ipv6 in internet of things: Analysis, experimentations and optimizations. *Ad Hoc Networks*, 14:15–25, 2014.

[16] Sangook Moon. Design of a high-speed serial programming interface compatible with bluetooth embedded systems. 2015.

[17] Ammar Muthanna, Andrey Prokopiev, Alexander Paramonov, and Andrey Koucheryavy. Comparison of protocols for ubiquitous wireless sensor network. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2014 6th International Congress on*, pages 334–337. IEEE, 2014.

[18] Edewede Oriwoh, Paul Sant, and Gregory Epiphaniou. Guidelines for internet of things deployment approaches: The thing commandments. *Procedia Computer Science*, 21(0):122–131, 2013.

[19] D. Pan. A tutorial on mpeg/audio compression. *IEEE Multimedia*, 2:60–74, Summer 1995.

[20] Sean Smith. *Trusted computing platforms: design and applications*. Springer, 2013.

[21] Hui Suo, Jiafu Wan, Caifeng Zou, and Jianqi Liu. Security in the internet of things: A review. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, volume 3, pages 648–651, 2012. ID: 1.

[22] Blase Ur, Elyse McManus, Melwyn Pak Yong Ho, and Michael L. Littman. Practical trigger-action programming in the smart home. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, pages 803–812. ACM, 2014.

[23] Mark Weiser. The computer for the 21st century. *Scientific American*, 265(3):94–104, 1991.

[24] Huiqun Zhao and Biao Shi. *The Implementation of Electronic Product Code System Based on Internet of Things Applications for Trade Enterprises*, pages 1271–1279. Computer Engineering and Networking. Springer, 2014.